情報システムと リスクマネジメントの一考察

武　田　久　義

一．は　じ　め　に

人間や組織は，意識するとしないとにかかわらず，リスクへの対応を行っている。そして人間や組織のリスクへの対応に関する研究は，「リスクマネジメント」という一つの学問として展開されてきている。そしてこれまでのリスクマネジメントの研究領域においても，一定の成果が見られる。しかし，現在，社会が大きく変化しつつある。工業社会から情報社会への変化である。現在がこのような大転換期にあることは，筆者もこれまでしばしば述べてきたところであり，多くの者が認めているところでもある。大切なことは，社会が大きく変化するとそれにともなってリスクもまた，大きく変化するということである。当然，それまでと変わることなく存在し続けるリスクもある。また，新たに発生するリスクもあれば，以前とは形や性質を変えるリスクもある。リスクの変化に対応してリスクマネジメントも新たな展開が要求されてくることは，間違いない。本稿は，リスクマネジメントの新たな展開の一歩として，情報社会の基礎をなす情報システムに関連するリスクとその対策

キーワード：情報化社会，リスクマネジメント・プロセス，技術的リスク，
組織的リスク，社会的リスク

について考えてみようとするものである。

ところで，リスクおよびリスクマネジメントについては，これまで多くの先達によってそれぞれの見解が明らかにされてきている。とくにリスクについては，これをどのようにとらえるかについて，実に多くの見解がある。これに関する筆者の見解は，いずれ稿をあらためて提示するつもりであるが，ここではリスクについて簡単にふれておきたい。

筆者は「好ましくない事態にいたる可能性」を，リスクの中心に据えたい。そしてリスクマネジメントについて考える場合，リスクを何らかの主体から見たものとして取り扱うことになる。リスクマネジメントの主体としては，個人から国家や世界的機関等様々なレベルのものが考えられる。また，一つの企業においても，一部門からトップレベルにいたるまで，様々な主体が考えられる。したがって，いかなる主体に対しても共通に適応できるリスクマネジメント論を展開することが必要であると思われる。本稿では，あらゆる主体に共通に適用することが可能なリスクマネジメントの一般論を念頭に置いている。

本稿では，まず最初に，リスクマネジメントのプロセスに沿ってリスクマネジメントの一般的な説明を行う。次に，リスクマネジメントの主体として企業を念頭に置いて，企業の情報システムに関連するリスクとそのマネジメントについての考察を行う。

二．リスクマネジメントについて

最初にリスクマネジメントについて若干の検討を行なってみたい。前述したように，基本的にすべての個人や組織はリスクマネジメントの主体となることが可能である。そしてその主体を大雑把に類別するならば，①国家や国連等の世界的な組織および機関ならびに自治体等，②企業・非営利組織ならびにグループ等，③家庭や個人等に分けることができるだろう。

リスクマネジメントは基本的に次のプロセスに従って実施される[1)]。

①リスクの発見・確認

②リスクの分析・評価

③リスクの処理・制御

④再評価，実施

（一）

企業を例にとった場合，最初の①リスクの発見・確認においては，企業活動のどこにどのようなリスクが，どのような形で存在しているかを把握することが目的となる。この段階においては，様々な方法があり得る。

リスク発見のための情報源としては，組織内外からの情報を収集する。組織内部の情報源としては，①業務日誌，事故・障害報告書や各種の報告書，契約書，年次報告書，調査分析結果など，②ブレーンストーミングの結果，③インタビュー，アンケート調査の結果，④有識者の意見，助言などがある。そして，組織外の情報源としては，①公的機関，私的機関，報道機関，同業種・異業種組織が発表した各種の類似組織の事例調査文書（報告書・記録，調査分析結果など）や法的要求事項，②インタビュー，アンケート調査の結果，③地域の情報，④各種セミナー等の報告，⑤組織外の専門家（外部コンサルタント等）の活用等が考えられる[2)]。

リスクの発見・確認のプロセスでは，明確でないもの，予測や推定がはいったもの，条件がきびしいもの，規模が大きいもの，過去に経験や類例がないもの，契約条項に問題があるもの，不安に思うものなどをすべて文書に書き出す。

なお，リスクの発見においては以下の点に注意する必要がある[3)]。

1）リスクマネジメントのプロセスについては，いくつかの異なった説明が可能である。本稿では，社団法人日本損害保険協会安全防災部編の『企業のリスクマネジメントに関する調査・研究報告書』2001年を参考にしつつ，進めていく。

2）鈴木敏正＆ＲＭコンソーシアム21，『この一冊ですべてがわかる　リスクマネジメントシステム』2002年，日刊工業新聞社，96頁。財団法人日本情報処理開発協会，『情報リスクに関するリスクマネジメント研究報告書』平成13年，インターネット版，５頁。

3）鈴木敏正＆ＲＭコンソーシアム21，前掲書，95頁。

①リスクに関する情報を提供した者が，不利益を被ることがないようにする。

②リスク発見は継続的に行う。そのためには監視，追跡が必要である。

③業務フロー分析，リスク発見シート等を活用する。

④組織の構成員のリスクを知覚する感性の向上をはかる。能力開発や教育を重視する。

⑤組織内外の先入観にとらわれない。第三者の助言も重視する。

リスクは状況に応じて変化するので，一度リスクを識別したらそれで終わりではなく，局面が変わるごとに識別しなおして，状況が変わるごとに確認する姿勢が大切である[4)]。

（二）

次のステップであるリスクの分析・評価においては，リスクの発生頻度，損失の程度および影響される範囲等を分析・評価する。発生頻度は，過去の実績ならびに統計等の一般的な資料を参考にして予測することになる。この場合，実際に事故は発生していなくともそのおそれがあったものも参考にする。損失の程度を評価する場合，損害の及ぶ範囲，賠償責任について評価することが重要である。

列挙されたそれぞれのリスクについて，リスクの発生頻度と損失の程度が次のように大雑把に分析・評価される。

Ａ．発生頻度は高い。損失も大きい。

Ｂ．発生頻度は低い。損失は大きい。

Ｃ．発生頻度は低い。損失は小さい。

Ｄ．発生頻度は高い。損失は小さい。

すべてのリスクを同一基準で算定する方法はない[5)]。そしてまた，リスクの正確な分析・評価は非常に困難である。これは，リスクの本質が不確実性

4）若部一鷹・最相力，『リスク管理の秘訣』1995年，共立出版，84頁。
5）鈴木敏正＆ＲＭコンソーシアム21，前掲書，102頁。

であることに由来している。しかし，リスクの分析・評価はリスクの経営に対する影響度を把握して，その対策を立てるためのものであるから必ずしも数値で示す必要はない。実際，リスクの分析・評価は，客観的な数値や過去のデータを利用する他に，主観的な判断で行われている場合が多い[6]。

（三）

第三のステップである情報の処理・制御においては，分析・評価したそれぞれのリスクについて，様々なリスクマネジメント手段が採用される。主要な手段としては，回避，除去・軽減，転嫁，保有等がある。リスクの分析・評価においては，上述したＡからＤまでの四つの局面におけるリスク処理手段として，だいたいにおいて次のものが採用される。

Ａ．リスク回避。

Ｂ．リスクの除去・軽減と転嫁。転嫁の代表的なものが保険である。

Ｃ．リスク保有[7]。

Ｄ．リスクの除去・軽減と保有。

（四）

最後のステップであるリスクの再評価・実施においては，これまでに行ってきたことが適切であったかどうかについて，費用と効果のバランスを考慮しつつ，全体的な立場からの評価を行う。

主として，次の事項について検討する。

㈠リスクの発見および確認は，適切かつ十分であったか。

㈡分析・評価は正しかったか。

㈢リスク処理手段の選択および組合せが適切であったか。

㈣費用と全体との効果でバランスはとれていたか。

6）土田義憲，『実践ビジネス・リスク・マネジメント』平成14年，財団法人大蔵財務協会，35頁。

7）保有したリスクについては，その変化を継続的に監視，追跡する必要がある。

㈦以上のフィードバック。

この段階では，第三者による評価も重要である。第三者のほうが当事者よりも客観的な評価を行うことが可能な場合が多いからである。

以上，きわめて大雑把にリスク・マネジメントのプロセスについて述べてきた。以下，本稿では情報システムの導入と維持・管理に関連するリスクに絞って考察しよう。なお，基本的にあらゆるリスクマネジメントの主体を対象としているものの，主として企業を念頭に置きつつ考察を進めていくこととする。

三．情報システムのリスクマネジメント

(一)リスクの発見・確認

情報システムに関連するリスクは，システムの構築に伴い不可避的に発生する。それは，「情報技術（information technology：ＩＴ）が本来もつ特性（たとえば，情報はコード化され，記録は電磁的であること等）に起因して発生し，企業等の業務システムや管理システムの中に内在する」。通常，これらは「コントロールされているが，コントロールが無かったり弱いと，事故や犯罪が発生する」[8]。また，どのようなセキュリティ対策をこうじても限界がある。それは一つには，どのようなセキュリティ技術および製品を用いたとしても，それを無効にするようなもの，たとえば新たなウイルスが発生しているということである。そして二つには，セキュリティ製品や情報システムの管理担当者だけではリスクを防止することが不可能だからである[9]。

ところで，情報システムにおけるリスクは，一般的に次のような特徴を持っている[10]。

①情報そのものの価値が再作成ロードという時間単価や要員の人件費と一

8）松田貴典，『情報システムの脆弱性』1999年，白桃書房，１頁。
9）古川泰弘，『情報リスクマネジメント』，2002年，かんき出版，３頁。
10）財団法人日本情報処理開発協会，『JIPDEC リスクマネジメントシステム（JRMS）のあり方に関する研究（JRMS2002）』，平成14年，インターネット版，第二部，５頁。

致しない。つまり知的財産権が大きい。

②コピーが容易であり，コピーされるという事故に気づきにくい。

③改ざんや消去が簡単にできる。

④効率化がコンピュータの最大の効果であるため，一度業務停止を行うと，または誤った処理を行うと，その影響を受ける者が何万の単位にも発生し被害対象者数が飛躍的に増大する。また，事件発生に要する時間が短時間である。

⑤インターネットなどを通じ国際化しており，事件・事故が国際的に展開する。

⑥国際的な対応が求められるが，一方で法律が整備されておらず，複数国家間にまたがる場合などは，どの国の法律の適用を受けるかにも注意が必要である。

⑦データの作成，プログラムの作成，ユーザの利用，システムの運用など人的要素が大きい。

それでは，以下の四つの情報システムの要素にしたがってリスクを洗い出してみよう[11]。

（1）入力情報処理に関連するリスク

①入力作業のミスおよび入力する情報そのものの誤り。

②入力ができないリスク。

③適正な人以外の利用。

（2）情報処理プロセスに関連するリスク

①情報機器の故障。

②自然災害，火災等による業務停止。

③プログラムミスおよびソフトウェアにおける人的リスク[12]。

11）主に以下の文献を参考にした。財団法人日本情報処理開発協会，前掲『情報リスクに関するリスクマネジメント研究報告書』。松田貴典，前掲書。松倉正俊，『インターネット・セキュリティとは何か』2002年，日経ＢＰ社。

12）ソフトウェアの開発が人的で，時間，労力，能力，知力に依存していることから，ソフトウェアには人的ミスによる欠陥が存在するおそれがあるほか，ソフトウェ

④運用トラブル。

⑤設計そのもののミス。

⑥回線管理にともなうリスク。回線の切断や短時間のアクセス集中等による使用不能等の回線を利用することからくるリスク。

⑦データの消失のリスク。

⑧均一のデータエラーが大量に発生するリスク[13]。

⑨不正コピーや改ざん等のリスク。電磁的記録のため，痕跡を残さずにコピーや改ざん等を行うことができる。また，漏洩も行われる。そして結果的には，内部統制が欠如することにもなる。

⑩現場要員に端末の利用方法のみを教育することで，均一的なデータ処理はできても情報システムが故障した場合等は，誰も手作業処理ができず，ひたすら修復を待つことになる。

⑪オペレーション・ミスのリスク。

⑫情報システムに関する無知によるトラブル。

⑬リカバリの不備，業務継続計画の不備等，事件・事故が発生した後の対応の失敗もここに含まれる。

⑭一度情報が発信されると，コントロールできない状態でネットワークの中を駆けめぐるリスク。

（３）出力情報に関連するリスク

ここには価値有る情報の取扱いに関するリスクが含まれる。

①情報漏洩リスク。

②不正使用リスク。

（４）組織外情報リスク

①まず，以下のようなインターネットに関連した種々のリスクがある。

ａ．なりすまし

アの品質・生産性に個人差が大きくあらわれる。

13）ソフトウェアにはバグ（欠陥）が含まれていることが多い。間違って処理することや，情報を紛失したりする。処理プロセスは見えないため，後になって大量のエラーが発見される。

b．事後否認
c．データ破壊
d．ホームページの乗っ取り
e．不正アクセス
f．いたずらメール，メール爆弾
g．サイバーテロ

②ネットワークシステムの不稼働リスク。
③決済業務の停止・不能リスク。決済不能による連鎖倒産（システミックリスク）。
④時差による国際的な決済不能。
⑤プライバシーの侵害。
⑥アウトソーシング先の事件・事故。

次に，このようなリスクへの対処という観点から，以上見てきたリスク以外のリスクをも含めて，リスクを次の三つに整理してみる。

（1）基本的に技術的手段で対応する「技術的リスク」。
（2）従業員の教育を中心に，経営や組織のあり方に関する考慮を必要とする「組織的リスク」。リスクを包摂して，可能であればプラスに転化することが望ましい。
（3）単一の組織のみで対応することが困難で，主として社会全体として対応することが必要な「社会的リスク」。長期的には，病理の除去・改善が望まれる。

しかし，実際には多くのリスクはいずれの領域にも多少とも関連している。したがって，一般的にみてよりウエイトの高いと思われる方に分類した。それでは，これらそれぞれの側面ごとにリスクマネジメントについて若干の考察を行ってみよう。

（1）技術的リスク

すでに述べたように，情報技術の進歩とともにリスクそれ自体が変化する。

また，ソフトウェアの機能アップは，新たな欠陥を不断につくりだす。そのほか，情報システムやニューメディアを活用したニュービジネスが，たえず新たな事故を引き起こす[14]。このように，技術的リスクの発生は避けられない。

ここでは，以下のようにリスクを整理しておく。

①情報機器の故障。
②自然災害，火災等による業務停止。
③設計そのもののミス。
④回線管理にともなうリスク。
⑤データの消失のリスク。
⑥均一のデータエラーが大量に発生するリスク。
⑦なりすまし
⑧事後否認
⑨データ破壊
⑩ホームページの乗っ取り
⑪不正アクセス
⑫いたずらメール，メール爆弾
⑬サイバーテロ
⑭一度情報が発信されると，コントロールできない状態でネットワークの中を駆けめぐるリスク。

（２）組織的リスク

組織的側面におけるリスクとは，主として情報システムの専門性や組織の少数精鋭化によるブラックボックス化に関連したリスクであり，コンピュータがソフトウェアによって稼働する限り，このリスクは無くならない。このほか，情報システムにおける特性から生じる組織構成員の不正等もこのリス

14）松田貴典，前掲書，17頁。

クに含まれる。

①入力作業のミスおよび入力する情報そのものの誤り。

②入力ができないリスク。

③適正な人以外の利用。

③プログラムミスおよびソフトウェアにおける人的リスク。

④運用トラブル。

⑤不正コピーや改ざん等のリスク。

⑥情報漏洩リスク。

⑦不正使用リスク。

⑧故障した場合のリスク。

⑨オペレーション・ミスのリスク。

⑩情報システムに関する無知によるトラブル。

⑪事件・事故発生後の対応の失敗。

⑫アウトソーシング先の事件・事故。

⑬テクノストレスの発生。

⑭情報化投資と効果の関係が不明確になるリスク。これに関連して，情報化投資の妥当性が評価できず情報化投資が聖域化する。このことが様々な問題を引き起こす[15]。

⑮従来までのハイアラーキーな組織が情報社会に合わなくなるリスク[16]。

（3）社会的リスク

現在の社会は，企業等多くの組織や個人等が情報システムに大きく依存している。情報システムの高度化，社会化，国際化にともない，国家，企業，個人等々のそれぞれの相互の関係は非常に深まっている。それだけに，情報システムにおけるリスクの発生は，広範な影響を及ぼすことになる。主なリスクとしては，次のようなものが考えられる。

15）松田貴典，同書，24頁。
16）松田貴典，同書，92頁。

①インターネット犯罪の可能性。
②ネットワークシステムの不稼働リスク。
③決済業務の停止・不能リスク。決済不能による連鎖倒産。
④時差による国際的な決済不能。
⑤評判等の社会的評価の下落。

（二）リスクの分析・評価

前節で見たように，情報システムにおいては様々なリスクが発生する可能性がある。そこで，そのようなリスクの発生の可能性はどの程度であるのか，そしてリスクが発生した場合の損失はどの程度なのかという分析・評価が必要となる。

リスクの発生確率と損失の程度によって，ＡからＤの四つに大雑把に分類することについては，すでに述べた。しかし，場合によっては，必要に応じてさらに詳しい分析・評価が必要となる。一例を示しておこう[17]。

（１）リスク発生の確率

組織内部の情報源で把握可能なものは極力報告書などの記録や事実に基づいてその発生件数を把握する。一方自社では発生していないが，同業他社で発生したものや，有識者が指摘している，今後発生が予測されるリスクについては，それらの妥当性を判断して次のように自社の発生確率を評価する[18]。

①高い：ときどき発生。
②中程度：通常でない時に，一時的に発生する可能性がある。
③低い：通常はほとんど考えられない。緊急事態や人為的なミスが重なった場合に発生する可能性がある。

（２）損失の程度

当該組織におけるこれまでの実績，全国的統計，アンケート，ブレーンス

17）鈴木敏正＆ＲＭコンソーシアム21，前掲書，107頁を参考とした。
18）財団法人日本情報処理開発協会，前掲『情報リスクに関するリスクマネジメント研究報告書』，５頁。

トーミング，前例調査，業務プロセス分析等の様々なデータを総合的に考慮して，予想される損失の程度を決定する。いずれにせよ，高度な判断が要求されるところである。

①大：多大な影響があり，かつ長引く。

②中：一時的な影響があるが，時間をかければ修復可能。

③軽微：影響が小さく対処することが可能。

前節で分類した技術的リスク，組織的リスク，社会的リスクそれぞれのリスクについてリスクの発生確率と影響の大きさを決定したならば，これらがリスク分布図のどの位置にあるかを確かめて，リスクに関する全体の見取り図をつくる。

リスク分布図に従って，おおむね次のような処理計画がたてられることになる。

＊Ａ：臨時予算を確保し，最優先で対策を行う。

＊Ｂ：来年度予算の範囲で優先的に実施する。

＊Ｃ：中長期計画で検討し実施する。

＊Ｄ：当面，監視する。保有。

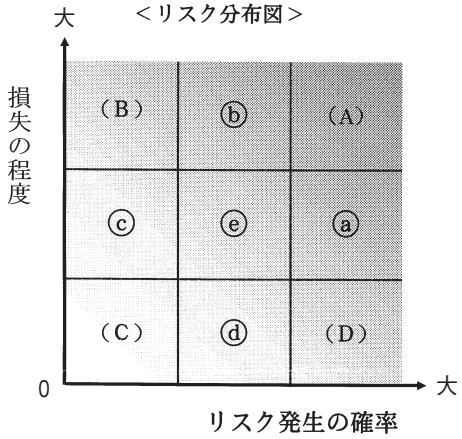
＊ａ，ｂ：年度予算の範囲で優先的に実施する。

＊ｃ，ｄ，ｅ：中長期計画で検討し実施する。

そしてこのような分析・評価に基づいて，以下のような処理が行われる。

(三)リスクの処理・制御

情報システムに関するリスク処理・制御は，すでに見たように回避，除去・軽減と転嫁，保有等を中心として展開される。しかし，現在の情報化の現状および将来の見通しを考えた場合，情報システムにおいては回避策は基本的に採用されるべきではない。それでは，たとえば情報に関連する知識やノウハウをほとんど全く持っていない企業等が情報システムを導入するかどうかの判断を迫られた場合には，どうすべきであろうか。もし組織改革や教育等についていかなる改革・改善を図ることなく情報システムを導入しても，



リスクの種類（前節のリスク）
（１）技術的リスク
①情報機器の故障。
②自然災害，火災等による業務停止。
③設計そのもののミス。
以下，省略。
（２）組織的リスク
①入力作業のミスおよび入力する情報そのものの誤り。
②入力ができないリスク。
③適正な人以外の利用。
以下，省略。
（３）社会的リスク
①インターネット犯罪の可能性。
②ネットワークシステムの不稼働リスク。
③決済業務の停止・不能リスク。決済不能による連鎖倒産。
以下，省略。

それはマイナスであろう。大きなリスクを抱え込むだけのことである。情報システムを導入する場合，それはメリットと同時にリスクをも受け入れる覚悟を持つことが必要である。そして情報システムを導入するならば，原則的には主体的な改革を行いつつ，アウトソーシングによって対応すべきであると思われる。そして，基本的にリスク回避を行うべきではないだろう。ただし，アウトソーシングを行う場合，危険な取引については回避することは，

当然である。

情報システムに関しては，ほとんどすべてのリスクは除去・軽減，転嫁ならびに保有の対象となるものである。以下では，除去・軽減を中心として，若干の考察を行ってみよう。

（1）技術的リスクの処理・制御

技術的リスクのうち，まず災害に関連したリスクについて考えてみる。災害とは，自然現象，過失，故意のいずれかの要因により，情報システムを構成する要素（人員，機器，アプリケーション，データ）に対して，損失事象を発生させるものである。災害の特徴としては，情報システムを構成する複数の要素に対して，同時に，かつ広範囲に影響を及ぼすことである。災害のタイプとしては，次の要因がある。自然要因には，落雷，雷鳴，風水害，豪雨，地震，鳥害，鼠害等がある。また人的要因としては，火災，爆発，漏水，停電等がある[19]。

そこで，災害に関連するリスクの対策としては，建物・施設の構造を災害に強いものにすることである。次に，万一の災害に備えてバックアップを行うことである。すなわち，本来のシステムが稼働不能になった場合でも応急に対処できるような態勢を整えておくことである。一般にハードウェアのバックアップとしては装置の二重化，回線の二重化，予備機の設置等がある。また，データ，プログラム等のバックアップには，ファイルの二重化等が考えられる。そして災害対策のバックアップとしては，当該情報システムから適当な距離を置いてバックアップしたものを次のようなかたちで保存しておく方法がある[20]。

①バックアップセンタ

ａ．遠隔地にハードウェアを含めて一式用意（自前，アウトソーシング）し，データはほぼ同期がとれた状態にしておく。

19）財団法人日本情報処理開発協会，同書，40頁。
20）財団法人日本情報処理開発協会，同書，23頁および53頁。

ｂ．遠隔地にディスク装置を用意し，ほぼ同期がとれた状態でリモートコピーする。

ｃ．他社または社内の他支店，他事業所のセンタ等，通常正常な情報処理が行われている同規模のセンタと相互バックアップセンタ等の契約を交わす。データはリモートコピーまたはＭＴ等を持ち込む。（１日１回，災害時等）

②外部保管

１日４回，１日１回，週１回，月１回等の単位でデータをＭＴに取り，外部保管会社へ預ける。データはたとえば，全データ，重要データ，アプリケーションまで等とする。

次に，インターネットに関連したリスクについてみよう。

インターネットに関連したリスクの処理に関しては以下のような様々なセキュリティ対策技術が用いられる[21)]。

①監視：ネットワークを通して外部から入ってくる情報と外に出ていく情報を監視するものである。

②ログ取得：自己のサイトに出入りする交信を記録するもので，不正アクセスの事前防止機能を持つ。

③暗号化：盗聴防止手段としてまず最初に考えられるのが，暗号を使用することである。暗号化は，「公開鍵方式」によって事後否認を防止することも可能である。

④認証：インターネット上の相手について，実在するかどうか，相手の身元や権限等を判別するために，また，ひろくなりすましを防止するための方法として用いられる。このほか，メッセージそのものが改変されていないかどうかについても，確認することも行うことができる。

⑤アクセス・コントロール：ユーザーＩＤやパスワードの設定等により，資格を有する者にのみアクセスを認めるものである。

21）主に松倉正俊，前掲書を参考とした。

⑥ウイルス・チェック：コンピュータ・ウイルスに感染したファイルやメモリーをのウイルスを凍結したり，拡大を防いだり，消去したりするために，ソフトウェアをインストールするものである[22]。

以上のように，インターネットに関連するリスクの一定部分については，かなり有効な対策が可能である。しかし，個々の企業等の対策には，限界があることは明白である。

（2）組織的リスクの処理・制御

まず第一に，ブラックボックス化への対策である。これは主として，情報化投資を中心とした様々な情報関連領域が聖域化することへの対策である。これに対しては，まず第一に広く情報に関連する教育を行う必要がある。それと同時に，情報を専門に担当する以外の者にも理解できるような様々な工夫が必要である。

次に，内部の不正に関するリスクについてである。この問題は，とくに情報システムのみに関連するものではない。しかし，痕跡を残さずに処理できることから，情報システムにおいては不正コピー，改ざん，漏洩等がより容易に行われやすいことである。これに対しては，一つには，より厳重なチェックを行う等の方法が考えられる。これに関連しては，次のような対策が考えられる[23]。

①パソコンに内蔵された機密情報がパソコンとともに盗まれるのを防止するために，ＰＣの社外持ち歩きを制限する。

②どうしても持ち歩く場合は，ＰＣ内に秘密情報を保存しない。

③機密情報が入っているフロッピーディスクの保管手続きを定める。

④社内情報を整理・分類して，分類された情報ごとにアクセスできる人を制限する。

22）不断に新たなウイルスが誕生しているために，ウイルスをチェックするソフトウェアを絶えず更新する必要があり，かなり高価なものとなる。

23）土田義憲，前掲書，106頁を参考とした。

⑤私用メールやアダルト・サイトへのアクセスなど，業務以外の利用を禁止する。

⑥セキュリティ・ポリシーで従業員が守るべきセキュリティ条項を明らかにし，研修を通じて，その遵守を徹底させる。

最後に，そして最も大切なことは，情報教育および訓練を実施することである。そして教育・訓練には，次のような知識やスキルの習得が含まれている[24)]。

①リスクマネジメントの活動の重要性。

②リスクマネジメントの知識。

③リスクごとに直面する可能性がある状況を想定した教育・訓練。

このほか，ユーザーに対する教育も必要であろう。しかし，教育は以上のことに止まっているべきではないように思われる。情報システムに関連する教育は，いはばスキルだけではなく，そのベースにあるものが重要である。それはたとえば，事故の発生によって生じる不利益が，関係者，組織全体，さらには広く社会全体に及ぶものであることを，真に納得してもらうことである。それは，教育の目的とするものを各人が主体的に取り組むような環境を形成することである。そしてこのような職場環境の構築は，オペレーション・ミスを減らしたり，テクノストレスを減少させるための取組みとも通底するものである。そしてそれは，さらに従来のハイアラーキーな組織のあり方に関する問題とも関連してくる。このように，リスクマネジメントの観点からしても，情報社会においては経済的利益とは異なるもう一つの重要な課題が必要となってくるように思われる。

（３）社会的リスクの処理・制御

社会的リスクには，これまで見てきた技術的リスクや組織的リスク以外の広範なリスクが含まれる。しかし，主として法律・規則や倫理面に関するリ

24）鈴木敏正＆ＲＭコンソーシアム21，前掲書，58頁。

スクが対象となる。

企業にとって法律や倫理面で特に注意すべきことは，プライバシーの保護に関連することである。企業は，一般的にみて，顧客リストをはじめとする多くの個人情報を所有している。したがって，個人情報にアクセスできる担当者を制限する等，その使用においては細心の注意を払うほか，万一それが漏洩した場合の対策も十分に練っておく必要がある。しかし基本的な問題として，情報を取り扱う者としての最低限のマナー，広義の情報倫理を確立することが要求されると思われる。

また，他者に損害を与えた場合の対策としては，保険に加入することも一つの方法である。情報関連のリスクに対する保険としては，コンピュータ総合保険，ネットワーク保険，動産総合保険等がある。このほか，総合ＩＴリスク・ソリューションを提供する保険も市場に提供されている。それは，データやプログラムの損害に対する保障に加え，コンピュータ・ウイルスや不正アクセスが原因である場合のウイルス駆除費用，原因究明費用，再発防止対策費用，第三者への謝罪広告費等の対策費用をパッケージ化した保険である。またこれに加えて，データ復旧アシスタント・サービスやＩＴセキュリティ診断サービス（有料）も付加されている。

(四)再評価，実施

これまで見てきた数々のリスク処理手段やそのミックスが，結果としてリスクの抑止や損失の軽減に寄与したかどうかが評価される。この場合，リスクマネジメントの実施状況の妥当性について，方法と程度における適切性という二つの側面から検討される。この段階における基本は，次のことである。

すなわち，リスクの適切な把握と，リスクの発生に対する処理手段のミックスが十分に機能しているかどうかについての点検である。また，不十分ではなくても不必要になされていないかどうかについても，処理手段を具体的に検討してみる必要がある。そして結果的にみて，情報システムに関連するリスクの発生が未然に防げたならば，あるいは日常的な経営活動に大きな支

障を来すことなく損失を押さえることができたならば，それをもってリスクマネジメントはいちおう成功であったと評価すべきである。基本的にリスクマネジメントは，肥大化すべきではなく，縁の下の力持ちであるべきではないかと思われる[25)]。

前述した三つのリスクについて見た場合，主要な評価事項は次のものであろう。

（１）技術的リスク

①リスクの発見および確認は，適切かつ十分であったか。

②分析・評価は適切であったか。

③処理手段は有効に機能したか。

④費用をかけすぎることはなかったか。

（２）組織的リスク

①リスクの発見および確認は，適切かつ十分であったか。

②分析・評価は適切であったか。

③教育は適切になされたか。

④不正が行われないような職場環境がつくられているか。

⑤テクノストレスへの対策は適切になされているか。

⑥ポカミスへの対策は適切になされているか。

（３）社会的リスク

①リスクの発見および確認は，適切かつ十分であったか。

25）なお，筆者のこのような見解とは別に，リスクマネジメントのパフォーマンスと有効性を評価する方法もある。簡単に述べておこう。パフォーマンス評価においては，客観性，再現性，検証可能性，実行可能性等を中心に，プログラム・リスク対策実施の進捗度・組織における内部基準・関連する法規制ならびに規格・リスクコミュニケイションの実行度等が評価される。そしてシステムの有効性を高めるために，リスクマネジメント計画，リスク対策，リスクマネジメント・システムの体制・仕組みを見直し，是正・改善がどの程度必要か，必要であればどの領域かということを決定する素材を組織に提供する。（森宮康・中林真理子，「リスクマネジメントと経営倫理」（経営倫理実践研究センター，『経営倫理』No.17所収，27-28頁。財団法人日本情報処理開発協会，前掲『JIPDEC リスクマネジメントシステム（JRMS）のあり方に関する研究（JRMS2002）』，６頁。鈴木敏正＆ＲＭコンソーシアム21，前掲書，130頁以下等。）

②分析・評価は適切であったか。

③リスクに強い組織が形成されているか。

④社会全体から見た場合のリスク防止に向けて何らかの貢献ができているか。

以上のほかに，日常的なリスクに対しては対応ができていても，緊急時のリスクの発生に対しては十分がどうかについも点検する必要がある。たとえば地震が発生した場合の緊急時対策，復旧対策等である。

さて，企業の行うリスクマネジメントは，業種によって，また企業が提供するサービスの種類・質・量によって千差万別である。したがって，どの程度のリスクマネジメントが必要であるかは，それぞれの企業が主体的に判断するしかない。その場合の重要な基準の一つは，すでに述べた経済性である。セキュリティ対策のための費用が，それを実施することによって得られる利益を上回ることは，長期的には許されないだろう。しかし，セキュリティ対策の費用をどこまで含めるかということは，実際にはかなり困難である。たとえば，教育や訓練はセキュリティ対策の重要な一つであるが，それは単にセキュリティ対策のためのみではない。常識的には，セキュリティを考慮しなければ採用しないだろう対策の費用のみをセキュリティ費用とすることが妥当と思われる[26)]。個々の企業において，情報システムの関連する費用の何パーセントをセキュリティ費用にあてるという決定がなされることになるものと思われる。

四．む　す　び

将来，情報システムが個人，組織，国家等のあらゆる領域において，生産から消費にいたるすべての分野で大きな位置を占めることは避けられない。そしてすでに見てきたように，情報システムにともなうリスクが必然的に発生する可能性があることもまた，否定できない。本稿は，このような認識の

26）日本会計士学館編，『情報システムのセキュリティ対策』昭和61年，中央経済社，160頁。

もとに，主に企業を主体とした場合のリスクマネジメントについての考察を行ってきた。しかし，何度もふれたように，本稿での考察は基本的にあらゆる主体に対して妥当するものと考えられる。

ところで，リスクマネジメントの根本に存在するべきものは，リスクの抑制であろう。それは，可能なかぎりリスクの発生をゼロに近づけることであるし，リスクが発生した場合にも，それによって生じる損失をできるだけ小さくすることである。そしてこの観点から考えた場合，我々には大きな課題が課されているのではないかと思われる。それは，これまで見てきたように，情報システムに関連するリスクのかなり多くの部分が人間の行為と深い関連を有しているということである。したがって，情報システムにおけるリスクの研究は必然的に「人間」の研究に関連してくるものであろう。そしてそれは，情報化社会とはどのような社会であるのかという根源的な問題とも関連してくる。

今回，情報システムという，筆者が不得意とする分野の一つに挑戦することとなった。それは，将来の情報社会におけるリスクとそのマネジメントについて考えていくうえでどうしても避けて通ることができない問題であると考えたからである。しかし，情報システムそれ自体においても，すべての問題について検討することはできなかった。とくに，将来最も重要となると思われる情報倫理については，これを全面的に割愛せざるをえなかった。

このほか，思い違いやミスも多々おかしているかもしれない。大方のご指摘を望むしだいである。

（たけだ・ひさよし／経営学部教授／2002年10月31日受理）

A Study of Risk Management of Information Systems

Hisayoshi TAKEDA

In the information oriented society, we are confronted with new risks in addition to exisisting risks. This article intended to clarify the newly occurred risks related to information system, and to comment about risk management of information system.

In this article, the author classified risk management process in four steps as follows.

(1) The first step is the “confirmation of risks”.

(2) The second step is the “assessment of risks”.

(3) The third step is the “dealing with risks”.

(4) The fourth step is the “evaluation of practices”.

And risks relating to information system are classified into three types as follows.

(1) Technical risks.

(2) Risks concerned to organizations.

(3) Social risks.

After classificatin of main risks according to these three types, some methods of dealing with risks are delivered.